

Appl. No. 09/655,229
Response Dated March 17, 2005
Reply to Office Action dated January 18, 2005, Paper No. __

REMARKS

In view of the following remarks, the Applicant respectfully requests reconsideration of the present application.

Objection

The Office Action dated January 18, 2005, Paper No. __ objects to the oath or declaration alleging that it is defective. The Office Action alleges that the oath or declaration is defective because:

1. it does not identify the citizenship of each inventor;
and
2. it does not identify the city and either state or foreign country of residence of each inventor.

The Declaration Traverses Objection

The accompanying "Declaration of Donald E. Schreiber" establishes that the declaration included with this application when filed with the United States Patent and Trademark Office ("USPTO") on September 5, 2000, on the second page thereof, includes:

1. the citizenship of each inventor; and
2. identifies the city and either state or foreign country of residence of each inventor.

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. __

For the preceding reason, Applicant respectfully submits that the declaration as originally filed:

1. traverses the objection appearing in the January 18, 2005, Office Action; and
2. requests that the objection be withdrawn.

Claim Rejection

The Office Action dated January 18, 2005, Paper No. __ rejects claims 1-29 under 35 U.S.C. § 102(b) as being anticipated by United States Patent No. 5,804,703 entitled "Method and Apparatus for Digital Signature Authentication" which issued September 8, 1998, on an application filed by Richard E. Crandall ("the Crandall patent").

The Cited Reference

Applicant hereby incorporates by reference as though fully set forth here the analysis of the Crandall patent's disclosure which appears:

1. on pages 3-6 of the response received by the United States Patent and Trademark Office ("USPTO") on July 12, 2004, to a prior March 8, 2004, Office Action; and
2. on all seven (7) pages of Exhibit B to the response received by the United States Patent and Trademark Office

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

("USPTO") on July 12, 2004, to the prior March 8, 2004,
Office Action

**Legal Principles Applicable to
Rejections Under 35 U.S.C. 102(b)**

Certain well established principles are to be applied in assessing whether or not a reference anticipates a claim under 35 U.S.C. 102(b). First, the claims of a patent, which define the invention, are "to be construed in light of the specification and both are to be read with a view to ascertaining the invention." United States v. Adams, 383 U.S. 39, 49, 148 USPQ 479, 482 (1966). The "differences between the prior art and the claims at issue are to be ascertained." Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966). The prior art as a whole must be considered, and those portions of the prior art arguing against or teaching away from the claimed invention must be considered. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc., 796 F.2d 443, 448, 230 USPQ 416, 420 (Fed. Cir. 1986), In re Hedges, et al., 783 F.2d 1038, 1041, 228 USPQ 685, 687 (Fed. Cir. 1986).

[F]or anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. Manual of Patent Examining Procedure ("MPEP") Eighth Edition Revision 1, February 2003, § 706.02, p. 700-21 (Emphasis supplied)

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

"Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." Rockwell International Corporation v. The United States, 147 F.3d 1358, 1363, 47 USPQ2d 1027, 1031 (Fed. Cir. 1998) citing National Presto Indus. v. West Bend Co., 76 F.3d 1184, 1189, 37 USPQ2d 1685, 1687 (Fed. Cir. 1966). In determining anticipation under 35 U.S.C. § 102, functional language, preambles, and language in "whereby," "thereby," and "adapted to" clauses cannot be disregarded. Pac-Tec, Inc. v. Amerce Corp., 903 F.2d 796, ____, 14 USPQ2d 1871, 1876 (Fed. Cir. 1990).

Argument

Attached hereto as Exhibits A, B and C are charts respectively for independent claims 1, 10/19 and 28. Those charts compare claim element by claim element the text of the respective claim with:

1. the text appearing in the January 18, 2005, Office Action which alleges where the element appears in the Crandall patent;
2. the text excerpted from the Crandall patent which the January 18, 2005, Office Action alleges anticipates the claim element; and

3. Applicant's comments regarding the January 18, 2005, Office Action's allegation and/or the disclosure of the Crandall patent which is pertinent to the claim element. Applicant respectfully submits that attached claim charts of Exhibits A, B and C establish that independent claims 1, 10, 19 and 28 traverse rejection under 35 U.S.C. § 102(b) based upon the disclosure of the Crandall patent.

**The Crandall Patent Fails To
Disclose A Receiver That Stores
A Plurality of Public Quantities**

The January 18, 2004, Office Action, in addressing the arguments presented in a response received by the United States Patent and Trademark Office ("USPTO") on July 12, 2004, to the prior March 8, 2004, Office Action, states:

1. on page 11 thereof:

Crandall discloses the public source contains the public keys of the sender and receiver, which inherently discloses that the public keys are transmitted by the sender and receiver:

and

2. on pages 11 and 12 thereof:

Crandall reference discloses the plurality of public quantities in column 13 lines 9-18: the publicly known information such as the public keys, the initial point, the field Fpk, and the curve parameter "a". Therefore, the publicly known information is not only restricted to the public keys.

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

Admittedly the Crandall patent discloses that the public source 813 stores:

1. the sender's and receiver's public keys, i.e. respectively ourPub and theirPub; and
2. other data used in cryptographic communications, e.g. d_k , x_1 , y_1 , the field F_{p^k} , x_1 / Z , and "a."

The Crandall patent further discloses in column 8 at lines 1-23 that the sender and receiver respectively compute their respective public keys ourPub and theirPub.

Accepting for sake of argument the January 18, 2005, Office Action's statement that the Crandall patent implicitly discloses that the public keys are transmitted by the sender and receiver, Applicant is unable to find any disclosure in the Crandall patent that the receiver stores or transmits for storage any of the other quantities d_k , x_1 , y_1 , the field F_{p^k} , x_1 / Z , or "a" into or to the source 813. Stated in a slightly different way, the Applicant respectfully submits that the Crandall patent is totally silent about how or by what entity the other quantities d_k , x_1 , y_1 , the field F_{p^k} , x_1 / Z , or "a" get stored into the public source 813. Yes, the receiver might possibly store the other quantities d_k , x_1 , y_1 , the field F_{p^k} , x_1 / Z , or "a" into the source 813. However, so might the sender, or so might some other entity unidentified in the Crandall patent.

Pending independent claims 1, 10 and 19 all require not merely that a publicly accessible repository store a plurality of public quantities similar to the Crandall patent. Those claims all expressly require that the receiver transmit for storage in a publicly accessible repository a plurality of public quantities. As clearly established by the claim charts of Exhibits A and B for claims 1 and 10/19 attached to this response, at best the Crandall patent discloses implicitly that the receiver stores only a single quantity, i.e. its public key theirPub, into the source 813. Since the receiver's public key, theirPub, is a single quantity, Applicant respectfully submits that the Crandall patent fails to expressly or implicitly disclose, or to even suggest, that the receiver transmit a plurality of public quantities for storage in a publicly accessible repository.

As explained above, the Crandall patent's disclosure leaves for speculation how the quantities d_k , x_1 , y_1 , the field F_{p^k} , x_1 / Z , or "a" get stored into the public source 813. It is improper to reject claims under 35 U.S.C. § 102(b) based upon speculation, particularly a speculation that is influenced by reading the claims of a pending patent application. Because the Crandall patent fails to disclose or even suggest either expressly or implicitly that the receiver transmit for storage in a publicly accessible repository a plurality of public quantities as expressly required by the texts

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

of independent claims 1, 10 and 19, Applicant respectfully submits that those claims all traverse rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

The Applicant further observes that, as set forth in the claim chart of Exhibit C attached hereto, the preceding analysis of the Crandall patent's disclosure applies equally to independent claim 28's express requirement that the sender store a plurality of quantities in a publicly accessible repository. Accordingly, because the Crandall patent fails to disclose or even suggest either expressly or implicitly that the sender transmit for storage in a publicly accessible repository a plurality of public quantities as expressly required by the text of independent claim 28, Applicant respectfully submits that the claim also traverses rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

**The Crandall Patent Fails
To Disclose Claim 10's
Key Exchange Activities**

Section (2) of independent claim 10's element i., and section (1) of that claim's element ii. both expressly encompass pre-cryptographic communication activities which occur while computing an encrypting and decrypting key. As set forth in the January 18, 2005, Office Action on pages 6 and 7 and in the excerpts from the Office Action appearing in the chart of Exhibit B for independent

claim 10 attached hereto, the Office Action alleges that post key exchange cryptographic communication activities disclosed in the Crandall patent, i.e. exchanging a cyphertext message and signature, disclose the pre-cryptographic communication activities encompassed:

1. by section (2) of independent claim 10's element i.; and
2. by section (1) of that claim's element ii.

The Applicant respectfully submits that the post key exchange cryptographic communication activities of exchanging a cyphertext message and signature do not anticipate pre-cryptographic communication activities which occur while establishing an encrypting and decrypting key. Because the Crandall patent fails to disclose or even suggest either expressly or implicitly the subject matter encompassed by section (2) of independent claim 10's element i. and by section (1) of that claim's element ii which are required by the text of independent claim 10, Applicant respectfully submits that for this second reason claim 10 traverses rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

At the top of page 6, the Office Action applies the same claim rejection both to independent claims 10 and 19. Accordingly, because the Crandall patent fails to anticipate independent claim 10 for the reasons set forth in the preceding paragraph, for that

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

same reason independent claim 19 also traverses, in a second way, rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

**The Crandall Patent Fails
To Disclose Elements of
Digital Signature Claim 28**

In addition to failing to disclose that the sender stores a plurality of public quantities in a publicly accessible repository as required by the preamble of independent claim 28, as established by the claim chart of Exhibit C the Crandall patent also fails to disclose:

1. evaluating expressions of at least two (2) different verification relationships; and
2. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.

The Crandall patent discloses computing a point on a curve in two different ways, i.e. point Q and the point R. In the terminology of the present application appearing beginning on page 22 at line 14, computing the points Q and R constitutes evaluating expressions of a single verification relationship. As set forth below in the terminology of the present application, the Crandall patent then compares the points Q and R to determine whether they match.

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

$$u^o(X_1 / 1) = Q \quad \neq \quad R = P + M(\text{ciphertext}, P)^o\text{ourPub}$$

If the points Q and R match, the digital signature is authenticated. Thus, as shown above, in the terminology of the present application, the Crandall patent discloses an operation similar to that of either verification relationship no. 1 or verification relationship no. 2 which appear on page 22 of the present application.

For the preceding reasons, the Crandall patent does not, in the terminology of the present application, disclose nor does it suggest comparing the results obtained by evaluating expressions of at least two (2) different verification relationships. Because the Crandall patent fails to disclose or even suggest comparing the results obtained by evaluating expressions of at least two (2) different verification relationships which the text of independent claim 10 expressly requires, Applicant respectfully submits that for this second reason claim 28 traverses rejection under 35 U.S.C. § 102(b) based upon the Crandall patent.

Conclusion

Since as analyzed above and on the attached claim charts the Crandall patent fails to disclose storage of any information or data other than ourPub and theirPub into the "public source 813"

Appl. No. 09/655,229

Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

respectively by a sender 801 or 1201 or by a receiver 802 or 120, independent claims 1, 10, 19 and 28 traverse rejection under 35 U.S.C. § 102(b) based upon that reference.

Furthermore, independent claims 10 and 19 also traverse rejection under 35 U.S.C. § 102(b) based upon the Crandall patent for a second reason because post key exchange cryptographic communication activities of exchanging a cyphertext message and signature do not anticipate pre-cryptographic communication activities which occur while establishing an encrypting and decrypting key.

Lastly, independent claim 28 also traverses rejection under 35 U.S.C. § 102(b) based upon the Crandall patent for a second reason because, in the terminology of the present application, the Crandall patent discloses evaluating and comparing expressions of a single verification relationship rather than the at least two (2) verification relationships expressly required by claim 28's text.

///

///

///

///

///

///

///

Appl. No. 09/655,229

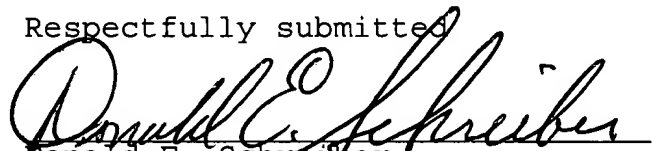
Response Dated March 17, 2005

Reply to Office Action dated January 18, 2005, Paper No. ____

For the preceding reasons, Applicant respectfully:

1. submits that pending independent claims 1, 10, 19 and 28, together with claims 2-9, 11-18, 20-27 and 29 depending respectively therefrom, are allowable over the Crandall patent;
2. requests that the rejection of claims 1-29 under 35 U.S.C. § 102(b) based upon that reference be withdrawn; and
3. requests that this patent application pass promptly to issue.

Respectfully submitted


Donald E. Schreiber
Reg. No. 29,435

Dated: 17 March, 2005

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicant

Claim Text

Office Action

US 5,805,703

Applicant's Comment

1. In a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted cyphertext message "M" obtained by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device, and

in which a receiving cryptographic unit "R" receives the cyphertext message M from the communication channel I and by supplying the cyphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom

a method by which the units S and R mutually establish a cryptographic key K by first exchanging messages before the sending unit S transmits the cyphertext message M comprising the steps of:

Application/Control no: 09/655,229
Docket no. 2174

-1-

Claim 1
March 16, 2005

a. the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities;

Crandall: column 20 lines 15-24 and figure 12: store publicly known information

A separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 1201 and receiver 1202, the initial point (x_1, y_1) , the field F_p , and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may be transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively.

This text from the Crandall patent is ambiguous about whether the receiver transmits a plurality of quantities that are stored in the source 813.

However, the text of the Crandall patent beginning in column 8 at lines 1-23 as excerpted below discloses that the receiver publishes only one quantity, i.e. theirPub.

In the following description, the terms "our" and "our end" refer to the sender. The terms "their" and "their end" refer to the receiver. This convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and receivers, respectively. The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.

Step 301

At our end, a public key is computed:

ourPub $\in F_p$

ourPub = (ourPri) a (x_1, y_1) Equation (12)

Step 302

At their end, a public key is computed:

theirPub $\in F_p$

theirPub = (theirPri) a (x_1, y_1) Equation (13)

Step 303

The two public keys ourPub and

theirPub are published, and therefore

known to all users. (Emphasis supplied.)

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>b. the sending unit S:</p> <p>i. retrieving the plurality of public quantities from the publicly accessible repository;</p>	<p>Crandall: column 13 lines 18-30 and figure 12: the sender uses public storage information to generate key</p>	<p>In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, $ourPri$, is provided to the elliptic multiplier 805, along with the sender's public key, $theirPub$. The elliptic multiplier 805 computes an enciphering key e_k from $(ourPri)^2(theirPub) \pmod p$. The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message P_{txt}. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816.</p>	<p>Applicant is unable to find any disclosure in the Crandall patent that the receiver stores any other quantities, e.g. d_k, x_1, y_1, the field F_p, x_1/Z, p, or a, into the source 813.</p> <p>This text from the Crandall patent discloses that the sender retrieves only one quantity, i.e. $theirPub$, from the source 813.</p>
--	--	---	--

- ii. using at least some of the plurality of public quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities; and

Crandall: column 19: lines 42-48: plurality of sender's quantities are ciphertext message and signature)

A sender, represented by the components within dashed line 1201, encrypts a plaintext message Pxt to a ciphertext message C and generates a signature (u, P). This message C and signature (u, P) is sent to a receiver, represented by the components within dashed line 1202. The receiver 1202 decrypts the ciphertext message C to recover the plaintext message, and authenticates the signature (u, P).

Because, as set forth above, a sender retrieves only a single quantity, i.e. theirPub, from the source 813, the sender cannot use "some of the plurality of public quantities" in "computing and transmitting to the receiving unit R a plurality of sender's quantities."

The "plurality of sender quantities" recited in this claim element function similarly to the single quantity ourPub that the Crandall patent discloses. The text of the Crandall patent beginning in column 8 at lines 1-23 as excerpted below discloses that the sender publishes only a single quantity, i.e. theirPub.

In the following description, the terms "our" and "our end" refer to the sender. The terms "their" and "their end" refer to the receiver. This convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and receivers, respectively. The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.

Step 301

At our end, a public key is computed:

$$\text{ourPub} \in F_p^*$$

$$\text{ourPub} = (\text{ourPri})^*(x_1, y_1) \quad \text{Equation (12)}$$

Claim Text

Office Action

US 5,805,703

Applicant's Comment

			<p>In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, $ourPri$, is provided to the elliptic multiplier 805, along with the sender's public key, $theirPub$. The elliptic multiplier 805 computes an enciphering key e_k from $(ourPri)^{(theirPub)} \pmod{p}$. The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message $Ptxt$. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816.</p>	<p>Step 302 At their end, <u>a public key is computed:</u> $theirPub \in F_p^k$ $theirPub = (theirPri)^{x_i} \pmod{y_i}$ Equation (13) Step 303 <u>The two public keys $ourPub$ and $theirPub$ are published, and therefore known to all users.</u> (Emphasis supplied.)</p>
<p>iii. using at least one of the plurality of public quantities, computing the key K; and</p>	<p>Crandall: column 13 lines 18-30</p>		<p>This text from the Crandall patent discloses that the sender uses only one quantity, i.e. $theirPub$, from the source 813 in computing the sender's encrypting key K.</p>	

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>c. the receiving unit R, using at least one of the plurality of sender's quantities received from the sending unit S computing the key K.</p>	<p>Grandall: figure 12 and column 20 lines 42-52: the using sender's public key to compute deciphering key.</p>	<p>The receiver 1202 generates a deciphering key D TheirPri is provided from the private key source 808 to the elliptic multiplier 806, along with sender's public key, ourPub, (from the public source 813). Deciphering key D_k is generated from (theirPri)^e(ourPub) (mod p). The deciphering key D_k is equal to the enciphering key e_k due to the abelian nature of the elliptic multiplication function. Therefore, the receiver 1202 reverses the encryption scheme, using the deciphering key D_k, to recover the plaintext message from the ciphertext message C.</p>	<p>This text from the Crandall patent discloses that the receiver retrieves and uses only one quantity, i.e. ourPub, from the source 813 in computing the receiver's decrypting key .</p>
---	---	--	---

<p>10. A system adapted for communicating as an encrypted cyphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:</p>				
<p>a. a communication channel I adapted for transmitting the cyphertext message M;</p>		Crandall: summary: conventional cryptographic communication		The Crandall patent discloses a communication channel I.
<p>b. a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the cyphertext message M from one transceiver to the other transceiver via said communication channel I; and</p>		Crandall: summary: conventional cryptographic communication		The Crandall patent discloses a pair of transceivers.
<p>c. a pair of cryptographic units each of which is respectively coupled to one of said transceivers for transmitting the cyphertext message M thereto or receiving the cyphertext message M therefrom, each cryptographic unit:</p>		Crandall: summary: conventional cryptographic communication		The Crandall patent discloses a pair of cryptographic units.

i. when the cryptographic unit is to receive the cyphertext message M:

(1) storing plurality of public quantities in a publicly accessible repository;

Crandall: column 20 lines 15-24 and figure 12: store publicly known information

A separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 1201 and receiver 1202, the initial point (x_1, y_1) , the field F_p , and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may be transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively.

This text from the Crandall patent is ambiguous about whether the receiver transmits a plurality of quantities that are stored in the source 813.

However, the text of the Crandall patent beginning in column 8 at lines 1-23 as excerpted below discloses that the receiver publishes only one quantity, i.e. theirPub.

In the following description, the terms "our" and "our end" refer to the sender. The terms "their" and "their end" refer to the receiver. This

convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and receivers, respectively. The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.

Step 301

At our end, a public key is computed:

$\text{ourPub} \in F_p^*$

ourPub = (ourPri)^a (x₁, y₁) Equation (12)

Step 302

At their end, a public key is computed:

$\text{theirPub} \in F_p^*$

theirPub = (theirPri)^a (x₁, y₁) Equation (13)

<p>(2) receiving via the communication channel i a plurality of sender's quantities from a sending cryptographic unit, and</p>			<p>Step 303 <u>The two public keys $ourPub$ and $theirpub$ are published, and therefore known to all users.</u> (Emphasis supplied.)</p> <p>Applicant is unable to find any disclosure in the Crandall patent that the receiver stores any other quantities, e.g. d_k, x_1, y_1, the field F_{p^k}, x_1/z, p, or a, into the source 813.</p>
	<p>Crandall: column 19: lines 42-48 and figure 12: plurality of sender's quantities are ciphertext message and signature</p>	<p>A sender, represented by the components within dashed line 1201, encrypts a plaintext message P_{txt} to a ciphertext message C and generates a signature (u, P). This message C and signature (u, P) is sent to a receiver, represented by the components within dashed line 1202. The receiver 1202 decrypts the ciphertext message C to recover the plaintext message, and authenticates the signature (u, P).</p>	<p>The text of this claim element i. expressly establishes that sections (1) and (2) thereof occur during computation of the cryptographic key K when the cryptographic unit is to receive the ciphertext message. Transmission of a ciphertext message and signature, alleged in the Office Action as disclosing this portion of claim element i., occur later after a cryptographic key K has been established during an encrypted communication.</p> <p>In this claim 10, element iii. rather than this claim element i. encompasses sending the ciphertext message.</p> <p><u>Consequently, the Crandall patent's disclosure regarding sending both a ciphertext message and signature necessarily fails to disclose activity which occurs before a ciphertext message is sent, i.e. while establishing the cryptographic key K to be used during an encrypted communication.</u></p>

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>using at least one of the plurality of sender's quantities in computing the key K; and</p>	<p>Crandall: column 13 lines 18-30</p>	<p>In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, $ourPri$, is provided to the elliptic multiplier 805, along with the sender's public key, $theirPub$. The elliptic multiplier 805 computes an enciphering key e_x from $(ourPri)^{theirPub} \pmod p$. The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message P_{txt}. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816.</p>	<p>This text from the Crandall patent discloses that the receiver uses only one quantity, i.e. $theirPub$, from the source 813.</p>
--	--	---	--

Claim Text

Office Action

US 5,805,703

Applicant's Comment

ii. when the cryptographic unit is to send the ciphertext message M, retrieving the plurality of public quantities from the publicly accessible repository and using:

Crandall: column 13 lines 18-30 and figure 12: the sender uses public storage information to generate key

In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, $ourPri$, is provided to the elliptic multiplier 805, along with the sender's public key, $theirPub$. The elliptic multiplier 805 computes an enciphering key e_k from $(ourPri)^{(theirPub)} \pmod{p}$. The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message P_{txt} . The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816.

This text from the Crandall patent discloses that the sender retrieves only one quantity, i.e. $theirPub$, from the source 813.

Claim Text

Office Action

US 5,805,703

Applicant's Comment

(1) at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit; and

Crandall: column 19, lines 42-48: plurality of sender's quantities are ciphertext message and signature

A sender, represented by the components within dashed line 1201, encrypts a plaintext message Ptxt to a ciphertext message C and generates a signature (u, P). This message C and signature (u, P) is sent to a receiver, represented by the components within dashed line 1202. The receiver 1202 decrypts the ciphertext message C to recover the plaintext message, and authenticates the signature (u, P).

The text of this claim element ii. expressly establishes that section (1) thereof occurs during computation of the cryptographic key K "when the cryptographic unit is to send the ciphertext message". Transmission of a ciphertext message and signature, alleged in the Office Action as disclosing this portion of claim element ii., occur later after a cryptographic key K has been established during an encrypted communication.

In this claim 10, element iii. rather than this claim element ii. encompasses sending the cyphertext message.

Consequently, the Crandall patent's disclosure regarding actually sending both a cyphertext message and signature necessarily fails to disclose activity which occurs before a cyphertext message is sent, i.e. while establishing the cryptographic key K to be used, during an encrypted communication.

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>(2) at least one of the plurality of public quantities in computing the key K; and</p>	<p>Crandall: column 13 lines 18-30</p>	<p>In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission. The private key of the sender, $ourPri$, is provided to the elliptic multiplier 805, along with the sender's public key, $theirPub$. The elliptic multiplier 805 computes an enciphering key e_k from $(ourPri)^{(theirPub)} \pmod{p}$. The enciphering key is provided to the encryption/decryption means 803, along with the plaintext message P_{txt}. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The ciphertext message is transmitted to the receiver 802 over a nonsecure channel 816.</p>	<p>This text from the Crandall patent discloses that the sender uses only one quantity, i.e. $theirPub$, from the source 813.</p>
---	--	---	--

iii. including a cryptographic device having:	(1) a key input port for receiving the key K from the cryptographic unit;	Crandall: figure 12 and column 20 lines 25-41: the cryptography device is provided the key	In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission, as described above. The enciphering key is provided to the encryption/decryption means 1203, along with the plaintext message. The enciphering key is used with an encrypting scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The random number generator 1205 generates random number m and provides it to elliptic multiplier 805. Elliptic multiplier 805 generates point u and provides it to the receiver via nonsecure channel 816. The ciphertext message C is provided to the hasher 1207, along with the random number m and ourPri. Hasher 1207 generates point P and provides it to nonsecure channel 816. The ciphertext message, along with signature (u, P), is transmitted to the receiver 1202 over a nonsecure channel 816.	This text in the Crandall patent discloses that the encryption/decryption means 1203 receives the enciphering key.
---	---	--	---	--

Claim Text

(2) a plaintext port:

Office Action

Crandall: figure 12 and column 20 lines 25-41: the cryptography device is provided key along with plaintext

US 5,805,703

Applicant's Comment

This text in the Crandall patent discloses that the encryption/decryption means 1203 receives the plaintext message.

In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission, as described above. The enciphering key is provided to the encryption/decryption means 1203, along with the plaintext message. The enciphering key is used with an enciphering scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The random number generator 1205 generates random number m and provides it to elliptic multiplier 805. Elliptic multiplier 805 generates point u and provides it to the receiver via nonsecure channel 816. The ciphertext message C is provided to the hasher 1207, along with the random number m and ourPri. Hasher 1207 generates point P and provides it to nonsecure channel 816. The ciphertext message, along with signature (u, P), is transmitted to the receiver 1202 over a nonsecure channel 816.

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>(a) for accepting the plaintext message P for encryption into the cyphertext message M that is transmitted from the cryptographic device; and</p>	<p>Crandall: figure 12 and column 20 lines 25-41: generate ciphertext and send it</p>	<p>In operation, the sender and receiver generate a common one time pad for use as an enciphering and deciphering key in a secure transmission, as described above. The enciphering key is provided to the encryption/decryption means 1203, along with the plaintext message. The enciphering key is used with an enciphering scheme, such as the DES scheme or the elliptic curve scheme of the present invention, to generate a ciphertext message C. The random number generator 1205 generates random number m and provides it to elliptic multiplier 805. Elliptic multiplier 805 generates point u and provides it to the receiver via nonsecure channel 816. The ciphertext message C is provided to the hasher 1207, along with the random number m and ourPri. Hasher 1207 generates point P and provides it to nonsecure channel 816. The ciphertext message, along with signature (u, P), is transmitted to the receiver 1202 over a nonsecure channel 816.</p>	<p>This text in the Crandall patent discloses that the encryption/decryption means 1203 receives the plaintext message.</p>
<p>(b) for delivering the plaintext message P obtained by decrypting the cyphertext message M received by the cryptographic device; and</p>	<p>Crandall: column 20 line's 42-52 and figure 12</p>	<p>The receiver 1202 generates a deciphering key D TheirPri is provided from the private key source 808 to the elliptic multiplier 806, along with sender's public key, ourPub, (from the public source 813). Deciphering key D_k is generated from (theirPri)^{ourPub} (mod p). The deciphering key D_k is equal to the enciphering key e_k due to the abelian nature of the elliptic multiplication function. Therefore, the receiver 1202 reverses the encryption scheme, using the deciphering key D_k to recover the plaintext message from the ciphertext message C.</p>	<p>This text in the Crandall patent discloses that the receiver uses the deciphering key D_k to recover the plaintext message from the ciphertext message C.</p>

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>(3) a cyphertext port that is coupled to one of said transceivers:</p> <p>(a) for transmitting the cyphertext message M to such transceiver, and</p> <p>(b) for receiving the cyphertext message M from such transceiver.</p>	<p>Crandall: figure 12: the cryptography device sends the cyphertext</p> <p>Crandall: figure 12: the cryptography device receives the cyphertext</p>		<p>A text of the Crandall patent in column 12 at lines 51-57 describing FIG. 8 discloses that an encryption/decryption means 803 and 804 respectively located in a sender 801 and a receiver 802 respectively transmit and receive a cyphertext message C.</p>
--	--	--	--

<p>28. In a protocol for communication in which</p> <p>a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and,</p> <p>wherein before transmitting the message M and the digital signature, the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities,</p>	<p>Crandall: summary: communication channel; column 19 lines 42-48; send ciphertext and digital signature</p> <p>Crandall: column 20 lines 15-24: store publicly known information</p>	<p>A sender, represented by the components within dashed line 1201, encrypts a plaintext message Ptxt to a ciphertext message C and generates a signature (u, P). This message C and signature (u, P) is sent to a receiver, represented by the components within dashed line 1202. The receiver 1202 decrypts the ciphertext message C to recover the plaintext message, and authenticates the signature (u, P).</p> <p>A separate source 813 stores publicly known information, such as the public keys "ourPub" and "theirPub" of sender 1201 and receiver 1202, the initial point (x_1, y_1), the field F_p, and curve parameter "a". This source of information may be a published directory, an on-line source for use by computer systems, or it may be transmitted between sender and receiver over a non-secure transmission medium. The public source 813 is shown symbolically connected to sender 1201 through line 815 and to receiver 1202 and hasher 1206 through lines 814 and 1218 respectively.</p>	<p>The Crandall patent discloses a sender which transmits a cyphertext message together with a digital signature.</p> <p>This text from the Crandall patent is ambiguous about whether the sending unit S transmits a plurality of quantities that are stored in the source 813.</p> <p>However, the text of the Crandall patent beginning in column 8 at lines 1-23 as excerpted below discloses that the sender publishes only one quantity, i.e. ourPub.</p> <p>In the following description, the terms "our" and "our end" refer to the sender. The terms "their" and "their end" refer to the receiver. This convention is used because the key exchange of the present invention may be accomplished between one or more senders and one or more receivers. Thus, "our" and "our end" and "their" and "their end" refers to one or more senders and receivers, respectively. The public key exchange of the elliptic curve cryptosystem of the present invention is illustrated in the flow diagram of FIG. 3.</p>
---	--	---	--

<p>a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature</p> <p>comprising the steps performed by the receiving unit R of:</p>	<p>Crandall: column 16 lines 63-67: authenticate the digital signature</p>	<p>The receiver attempts to authenticate the signature by generating a pair of points to match the digital signature pair, using the ciphertext message and the public key of the purported sender. The receiver verifies the signature using the following steps:</p> <p>Step 301 At our end, <u>a public key is computed:</u> <u>ourPub</u> $\in F_p^k$ <u>ourPub</u> = (ourPri)^x(x₁, y₁) Equation (12)</p> <p>Step 302 At their end, <u>a public key is computed:</u> <u>theirPub</u> $\in F_p^k$ <u>theirPub</u> = (theirPri)^x(x₁, y₁) Equation (13)</p> <p>Step 303 <u>The two public keys ourPub and theirPub are published, and therefore known to all users.</u> (Emphasis supplied.)</p> <p>Applicant is unable to find any disclosure in the Crandall patent that the sender stores any other quantities, e.g. d_p, x₁, y₁, the field F_p, x₁, Z, p, or a, into the source 813.</p> <p>The Crandall patent discloses digital signature authentication.</p>
--	--	---

a. retrieving the plurality of public quantities from the publicly accessible repository;	Crandall: column 17 lines 1-50	<p>1) Using the u part of the signature, compute the point $Q = u^{\circ}(X_1 / 1)$</p> <p>2) Compare the point Q to the point $R = P + M(\text{ciphertext}, P)^{\circ} \text{ourPub}$</p> <p>The signature is invalid if these elliptic points Q and R do not compare exactly. In other words, if the signature is authentic, the following must hold: $u^{\circ}(X_1 / 1) = P + M(\text{ciphertext}, P)^{\circ} \text{ourPub}$</p> <p>Substituting for u on the left side of the equation above gives: $(m + \text{ourPri}^{\circ} M(\text{ciphertext}, P))^{\circ}(X_1 / 1) = P + M(\text{ciphertext}, P)^{\circ} \text{ourPub}$</p> <p>or: $m^{\circ}(X_1 / 1) + (\text{ourPri}^{\circ} M(\text{ciphertext}, P))^{\circ}(X_1 / 1) = P + M(\text{ciphertext}, P)^{\circ} \text{ourPub}$</p> <p>Substituting for ourPub on the right side of the equation yields: $m^{\circ}(X_1 / 1) + (\text{ourPri}^{\circ} M(\text{ciphertext}, P))^{\circ}(X_1 / 1) = P + M(\text{ciphertext}, P)^{\circ} \text{ourPri}^{\circ}(X_1 / 1)$</p> <p>Since $P = m^{\circ}(X_1 / 1)$ from above, the left side becomes: $P + (\text{ourPri}^{\circ} M(\text{ciphertext}, P))^{\circ}(X_1 / 1) = P + M(\text{ciphertext}, P)^{\circ} \text{ourPri}^{\circ}(X_1 / 1)$</p> <p>Moving ourPri in the right side of the equation gives: $P + \text{ourPri}^{\circ} M(\text{ciphertext}, P)^{\circ}(X_1 / 1) = P + \text{ourPri}^{\circ} M(\text{ciphertext}, P)^{\circ}(X_1 / 1)$</p>	<p>Applicant is unable to find anywhere in this text from the Crandall patent any description of retrieving a plurality of public quantities from a publicly accessible repository. Rather, this text from the Crandall patent describes mathematical computations performed in authenticating a digital signature.</p> <p>However, this text from the Crandall patent implicitly discloses that the receiving unit R retrieves the quantity ourPub and X_1 from the source 813.</p>
---	--------------------------------	--	---

Claim Text

Office Action

US 5,805,703

Applicant's Comment

<p>b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships; and</p>	<p>Crandall: column 17 lines 44-50: two different equations</p>	<p>Thus, a point on a curve is calculated via two different equations using the transmitted pair (u, P). It can be seen that by calculating Q from the transmitted point u, and by calculating R from transmitted point P, the ciphertext message, and the public key of the purported sender, the digital signature is assumed authenticated when Q and R match.</p>	
<p>c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.</p>	<p>Crandall: column 17 lines 49-50: the digital signature is assumed authenticated when Q and R match</p>	<p>Thus, a point on a curve is calculated via two different equations using the transmitted pair (u, P). It can be seen that by calculating Q from the transmitted point u, and by calculating R from transmitted point P, the ciphertext message, and the public key of the purported sender, the digital signature is assumed authenticated when Q and R match.</p>	<p>The text of the Crandall patent discloses computing a point on a curve, Q and R, via two different equations.</p> <p>Applicant is unable to identify anywhere in the text of the Crandall patent appearing in column 17 at lines 1-50 an evaluation of expressions of at least two (2) different verification relationships such as those disclosed in the present patent application beginning on page 22 at line 14..</p>
		<p>Thus, a point on a curve is calculated via two different equations using the transmitted pair (u, P). It can be seen that by calculating Q from the transmitted point u, and by calculating R from transmitted point P, the ciphertext message, and the public key of the purported sender, the digital signature is assumed authenticated when Q and R match.</p>	<p>The text of the Crandall patent discloses comparing Q and R which, in the context of the present application's disclosure appearing on page 22 beginning at line 14, constitutes only a single verification relationship.</p>